NCI-Frederick Account Lifecycle Management Practices
Version 1

National Cancer Institute - Frederick

November, 05, 2009
Approved on November, 05, 2009

For Official Use Only

TABLE OF CONTENTS

Record of Changes

Version Number	Release Date	Summary of Changes	Section Number / Paragraph Number	Changes Approved by and Date
1	11/05/09	Original		ITCC/ADWG

1. Purpose

This *NIH Account Lifecycle Policy* is established to effectively manage the establishment of user accounts for access to NIH Information Technology (IT) resources, the periodic review of user accounts and the closure of accounts upon an individual's termination or other departure.

2. Background

The NCI-Frederick Active Directory (AD) Organizational Unit (OU) resides within the NIH AD and is governed by NIH policy, procedure, guidelines, and practices. This NIH guidance includes the naming of AD objects (i.e., accounts and resources):

- No two NIH AD accounts shall be named the same; uniqueness enables the use of the user objects across multiple directories and applications.
- Organizations that participate in the NIH AD are required to standardize how they identify their AD network resources (e.g. Workstations, servers, printers, and domain controllers) when registering them in Domain Name System (DNS) and the NIH AD and to coordinate their standards with the Active Directory Operational Group (ADOG).
- Organizations are expected to adopt a network naming standard that is consistent and relevant to their operations but not infringing on other organizations naming standards.
- Organizations should consistently name AD network resources to reflect the organization they belong to. This is easily accomplished by using the IC acronym as a prefix to the identity of the network name.

The NCI-Frederick AD Naming Conventions will ensure compliance with NIH direction and guidance, create a consistent naming structure across NCI-Frederick AD accounts and resources, and support the mission of the NCI-Frederick access) and the directory information needed to associate individuals with account information. Furthermore, an "active" NED record shall be a prerequisite for granting access to NIH information systems and services. Granting of logical access to any IT resource must be tied to an identified sponsor through an authorization process and include an annual review of the need for on-going access. Deregistration of accounts must be properly managed to ensure privileges are revoked in a timely manner, or extended under strictly prescribed conditions.

The *NIH Account Lifecycle Policy* is set forth to be consistent with Federal requirements and supplements the DHHS *Information Security Program Policy*.

3. Scope

These practices apply to logical access accounts associated with NCI-Frederick users and resources. This includes employees, contractors, students, guest researchers, visitors, and others who access NCI-Frederick information systems and applications.
All accounts will be managed in accordance with NIH Account Lifecycle Management policy. As such, NED records shall be the authoritative source for all logical access at NIH.

Unless technically impossible, all NCI-Frederick related accounts should reside within the NCI-Frederick AD OU.

4. Policy

4.1 Primary User Accounts

Primary user accounts provide an authorized individual (employee, contractor, or recognized affiliate) access to IT resources. NED shall be used to associate individuals with all account assignments. In particular, the creation and deletion of primary user accounts must be associated with a single NED account provided by the users Adminstrative Officer (AO). In order to have a primary user account created within the NCI-Frederick AD OU the following is required:

- User must have active NED account;
- User must take NIH Information Security Awareness Training ;
- C&SS must be notified in writing (e-mail acceptable) by an authorized account sponsor (typically an AO or equivalent);
- User must agree to the NIH Information Technology General Rules of Behavior;
- Account must be associated with a single NED account;
- Account passwords must comply with NIH Password Policy.

User accounts must be reviewed at least annually to substantiate the continued need for the rights and privileges of the account.
User accounts are disabled within 24 hours after authorization for the account is revoked in NED or the NED record is deactivated. Disabled accounts will automatically be moved into a separate container. Disabled accounts are deleted after 15 days.

4.2 Secondary User Accounts

Secondary User Accounts:
Secondary user accounts provide an authorized individual (employee, contractor, or recognized affiliate) elevated administrative access to IT resources. NED is used to associate individuals with account assignments. In particular, the creation and deletion of secondary user accounts are associated with a single NED account and single primary user account. In order to have a secondary user account created within the NCI-Frederick AD OU the following is required:

- C&SS must be notified in writing (e-mail not acceptable) by NCI-Frederick ISSO;
- User must possess a valid primary user account;
- User must take required training for Secondary Accounts;
- Secondary account must be associated with a single primary user account and user's NIH ID;
- Secondary accounts are not authorized for normal web browsing;
- Secondary account cannot be "email enabled";
- Secondary account password must comply with NIH Password Policy.

4.3 Resource Accounts

Resource accounts are used to establish shared resources (such as a conference room, projector, mailbox, or other shared equipment) within the OU. In order to have a resource account created within the NCI-Frederick AD OU the following is required:

- C&SS must be notified in writing (e-mail acceptable) by a authorized account sponsor;
- Accounts must reside in the "Resource" subordinate OU with the NCI-Frederick OU;
- Accounts must exists in a "disabled" state;
- Accounts must have a 15 character password, but is exempt from the NIH Password Policy (in accordance with the NIH Account Lifecycle Policy).

4.4 Service Accounts:

Service accounts are interactive logins used by operating systems or applications to run a service or perform automated operations. In order to have a service account created within the NCI-Frederick AD OU the following is required:

- C&SS must be notified in writing (e-mail acceptable) by an authorized account sponsor;
- Accounts must reside in the "Service" subordinate OU with the NCI-Frederick OU;
- Account passwords must comply with NIH Password Policy; service accounts can be exempted from the 60 day password expiration policy with the approval of the NCI-Frederick ISSO and ADWG (in accordance with NIH Account Lifecycle Policy and NCI-Frederick Active Directory Guidelines).

4.5 Training Accounts:

Training accounts are logins used for classrooms and training purposes. In order to have a training account created within the NCI-Frederick AD OU the following is required:

- C&SS must be notified in writing (e-mail acceptable) by an authorized account sponsor;
- Accounts must have a 15 character password;
- Account passwords must be changed every 60 days.

5. References

1. Public Law 107-347 [H.R. 2458], The E-Government Act, Title II — Federal Management and Promote of Electronic Government Services, and Title III — Information Security Federal Information Security Management Act (FISMA) December 17, 2002.
2. NIH Account Lifecycle Management Policy; http://ocio.nih.gov/nihsecurity/NIH_Account_Lifecycle_Policy.doc
3. NIH Password Policy; http://ocio.nih.gov/nihsecurity/pwd_policy.pdf
4. NIH Rules of Behavior; http://ocio.nih.gov/security/nihitrob.html
5. NIH Information Security Awareness Training; http://irm.cit.nih.gov/nihsecurity/Final-InfoSecAwarenessTrainPol.doc
6. NIH FDCC Waiver Information ; http://irm.cit.nih.gov/security/FDCC_Waivers.doc

6. Information and Assistance

Comments, questions, suggestions or requests for further information should be directed to the ITCC and/or ADWG.

7. Glossary

Access Control — enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner (Defined in NIST SP 800-27, Appendix B).

Authorized Account Sponsor – a person identified as a responsible account requestor for a given system.

Authoritative source — the preeminent authority serving as the source of attributes or information that will be used by or linked to by other systems to associate users with accounts.

Authorization — the granting or denying of access rights to a user, program, or process (Defined in NIST SP 800-27, Appendix B).

Deregistration — the process of removing access rights by a recognized entity that manages those accounts.

HSPD-12 — An Executive directive for establishing a secure and reliable common identification standard for Federal employees and contractors.

Information Resources — information and related resources, such as personnel, equipment, funds, and information technology (Defined in 44 U.S.C., SEC. 3502).

Information Technology — any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources (Defined in 40 U.S.C., SEC. 1401).

Lifecycle — the concept of effectively managing a user account from creation through on-going review for continued need, to deregistration in a timely manner.

Logical access — the ability to interact with data through access control procedures such as identification, authentication and authorization.

NIH ID – also known as a NED number (xxx-xxxx-xxx)

Risk — the level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system

given the potential impact of a threat and the likelihood of that threat occurring (NIST SP 800-30, Rev A, Appendix E).

Rules of Behavior — the Rules hold users accountable for their actions and responsible for information security. Rules will clearly delineate responsibilities and expected behavior of all individuals. On an annual basis, all NIH users must read and electronically agree to abide by the NIH IT General Rules of Behavior. The Rules are included in the annual security awareness training. Systems may also have additional rules of behavior that are specific to that system.

Security Controls — the management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, adequately protect the confidentiality, integrity, and availability of the system and its information (Defined in NIST SP 800-53, Appendix B).

Sponsor/sponsorship — A sponsor substantiates the need for physical and logical access. At NIH the sponsor is an FTE Administrative Officer (AO) who is in the AO role in NED and has provided their Personal Identity Verification (PIV) Sponsor training certificate to the HSPD-12 Program Office. Before a sponsor can sponsor someone for physical and/or logical access, physical and/or logical access must be requested. This is done in NED by an Administrative Technician or AO.

User — person or process accessing an information system either by direct connections (that is, by way of terminals), or indirect connections (that is, prepare input data or receive output that is not reviewed for content or classification by a responsible individual).